10/802,165   - 2 -

In the Claims

1. (Original)   A method for communicating a secure electronic communication comprising:

generating a package using a non-browser application on a local computer, the package configured for electronic transmission that includes an electronic mail analogous interface, file data and an address associated with an addressee having a public electronic mail account;

communicating the package from the local computer to a secure server over a secure network connection over the public Internet;

storing the package at the server in association with the electronic mail account of the addressee;

communicating the package to the addressee;

decrypting the package; and

displaying the package to the addressee.

2. (Original)   The method of claim 1, further comprising encrypting the package at the local computer of a sender.

3. (Original)   The method of claim 2, wherein encrypting the package at the local computer of the sender further includes using a public key to encrypt the package.

4. (Original) The method of claim 1, wherein decrypting the package further includes using a private key associated with a public key previously used to encrypt the package.

5. (Original) The method of claim 1, further comprising storing the package as a draft package at the local computer prior to communicating the package to the secure server.

6. (Original) The method of claim 1, further comprising causing the addressee to be notified of the package using the public electronic mail account.

7. (Original) The method of claim 1, wherein communicating the package to the addressee further includes communicating the package using at least one of the secure network connection and a second secure network connection.

8. (Original) The method of claim 1, wherein generating the package further includes configuring the interface to be responsive to user input.

9. (Original) The method of claim 1, wherein generating the package further includes configuring the interface to display a status of the package.

10. (Original) The method of claim 1, wherein generating the package further includes adding additional file data to the package.

THIS PAGE BLANK (USPTO)

11. (Presently Amended)   The method of claim 1, wherein generating the package further

includes including a <u>Printer Control Language</u> (PCL) file within the file data.

12. (Original)   The method of claim 1, wherein displaying the package further includes

downloading the package from the secure server.

13. (Original)   The method of claim 1, wherein displaying the package further includes

automatically downloading the package from the secure server.

14. (Original)   The method of claim 1, further comprising compressing at least a portion of the

package.

15. (Original)   The method of claim 1, wherein communicating the package further includes

communicating the package over a https socket layer connection.

16. (Original) A method for communicating a secure electronic communication comprising:

generating at a local computer using a non-browser application configured for electronic transmission that includes an electronic mail analogous interface, an encrypted package comprising file data and an address associated with an addressee having a public electronic mail account; and

transmitting from the local computer the package over a secure network connection over the public Internet.

17. (Original) The method of claim 16, further comprising storing the package in association with an electronic mail account of the addressee.

18. (Original) The method of claim 16, further comprising communicating the package to the addressee.

19. (Original) A method for communicating a secure electronic communication comprising:

receiving over a secure network connection over the public Internet a package, using a non-browser application that includes an electronic mail analogous interface, the package configured for electronic transmission and comprising file data and an address associated with an addressee having a public electronic mail account, wherein the package has been stored remotely at a secure server;

decrypting the package; and

- 6 -

displaying the package to the addressee.

20. (Original) A method for communicating a secure electronic communication comprising:

generating a package for electronic transmission using a non-browser application that includes an electronic mail analogous interface;

encrypting the package;

communicating the package from the local computer to a secure server over a secure network connection over the public Internet wherein the package is stored at the server and communicated to an addressee; and

communicating a confirmation of delivery status of the package from the secure server to the non-browser application at the local computer via a secure network connection over the public Internet.

21. (Original) An apparatus comprising:

a local computer;

a server computer configured to communicate with the local computer over a secure network connection; and

program code in communication with at least one of the local and server computers, the program code configured to generate a package using a non-browser application on the local computer, the package being configured for electronic transmission that includes an electronic mail analogous interface, file data and an address associated with an addressee having

a public electronic mail account, the program code being further configured to communicate the package from the local computer to the secure server over the secure network connection, and to store the package at the server in association with the electronic mail account of the addressee, the program code being further configured to decrypt and communicate the package to the addressee.

22. (Original) The apparatus of claim 21, wherein the secure network connection includes a https socket layer connection.

23. (Original) The apparatus of claim 21, wherein the program code initiates encrypting the package at the local computer of a sender.

24. (Original) The apparatus of claim 23, wherein the program code initiates using a public key to encrypt the package.

25. (Original) The apparatus of claim 21, wherein the program code initiates using a private key associated with a public key previously used to encrypt the package.

26. (Original) The apparatus of claim 21, wherein the program code initiates storing the package as a draft package at the local computer prior to communicating the package to the secure server.

PAGE 10/19 * RCVD AT 10/22/2007 10:23:04 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-3/20 * DNIS:2738300 * CSID:15137720052 * DURATION (mm-ss):07-00

27. (Original) The apparatus of claim 21, wherein the program code initiates causing the addressee to be notified of the package using the public electronic mail account.

28. (Original) The apparatus of claim 21, wherein the program code initiates communicating the package to the addressee using at least one of the secure network connection and a second secure network connection.

29. (Original) The apparatus of claim 21, wherein the interface is configured to display a status of the package.

30. (Presently Amended) The apparatus of claim 21, wherein the file data includes a <u>Printer Control Language (PCL)</u> file.

31. (Original) The apparatus of claim 21, wherein the program code initiates automatically downloading the package from the secure server.

32. (Original) The apparatus of claim 21, wherein the program code initiates compressing at least a portion of the package.

33. (Original) An apparatus comprising:

       a computer; and

program code in communication with the computer, the program code using a

non-browser application and including an electronic mail analogous interface configured to

receive from a remote computer over a secure network connection over the public Internet an

encrypted package comprising file data and an address associated with an addressee having a

public electronic mail account, the program code being further configured to store the package in

association with an electronic mail account of the addressee and to communicate the package to

the addressee.

34. (Original) An apparatus comprising:

    a computer; and

    program code in communication with the computer, the program code configured

to receive over a secure network connection over the public Internet a package generated using a

non-browser application that includes an electronic mail analogous interface, the package being

configured for electronic transmission and comprising file data and an address associated with an

addressee having a public electronic mail account, wherein the package has been stored remotely

at a secure server, the program code further configured to decrypt and display the package.

35. (Original) An apparatus comprising:

    a computer; and

    program code in communication with the computer, the program code configured

to generate a package using a non-browser application that includes an electronic mail analogous

interface, the package being configured for electronic transmission, the program code further

being configured to encrypt the package and to communicate the package from the computer to a

secure server over a secure network connection over the public Internet, wherein the package is

stored at the server and communicated to an addressee, wherein the program code is further

configured to communicate a confirmation of delivery status of the package from the secure

server to the non-browser application at the local computer via a secure network connection over

the public Internet.

36. (Original) A program product, comprising:

        program code in communication with at least one of a local and a server

computer, the program code configured to generate a package using a non-browser application

that includes an electronic mail analogous interface on the local computer, the package being

configured for electronic transmission comprising file data and an address associated with an

addressee having a public electronic mail account, the program code being further configured to

communicate the package from the local computer to the secure server over a secure network

connection, and to store the package at the server in association with the electronic mail account

of the addressee, the program code being further configured to decrypt and communicate the

package to the addressee; and

        a signal bearing medium bearing the program code.

10/802,165   - 11 -   ELYN/10

37. (Original) The program product of claim 36, wherein the signal bearing medium includes at

least one of a recordable medium and a transmission-type medium.